



RECEIVED
RECEIVED
JUL 18 2001
JUL 18 2001
Technology Center 2600
G.O.L. 2100 PATENT

2131#5

I hereby certify that on the date specified below, this correspondence is being deposited with the United States Postal Service as first-class mail in an envelope addressed to the Commissioner for Patents, Washington, DC 20231.

July 12, 2001

Date

Sandy Reisman
Sandy Reisman

RECEIVED

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

JUL 18 2001

G.O.L. 2100

Applicant : C. Andrew Neff
Application No. : 09/816,869 Confirmation No.: 6077
Filed : March 24, 2001
For : VERIFIABLE, SECRET SHUFFLES OF ENCRYPTED DATA,
SUCH AS ELGAMAL ENCRYPTED DATA FOR SECURE
MULTI-AUTHORITY ELECTIONS

Art Unit : 2131

Docket No. : 324628002US3

Date : July 11, 2001

Commissioner for Patents
Washington, DC 20231

TRANSMITTAL OF INFORMATION DISCLOSURE STATEMENT

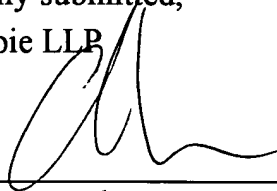
Sir:

In accordance with 37 C.F.R. §§ 1.56 and 1.97 through 1.98, applicant wishes to make known to the Patent and Trademark Office the references set forth on the attached form PTO/SB/08A (copies of the cited references, as required under 37 C.F.R. § 1.98, are enclosed). Although the aforesaid references are made known to the Patent and Trademark Office in compliance with applicant's duty to disclose all information of which he is aware that is believed relevant to the patentability of the above-identified application, applicant believes that his invention is patentable. As to any document

supplied, applicant does not admit that it is "prior art" under 35 U.S.C. §§ 102 or 103, and specifically reserves the right to antedate any such document, as by a showing under 35 C.F.R. § 1.131 or other method.

Please acknowledge receipt of this Information Disclosure Statement and kindly make the cited references of record in the above-identified application.

Respectfully submitted,
Perkins Coie LLP



Christopher J. Daley-Watson
Registration No. 34,807

CJD:SBR
Enclosures:
Postcard
Form PTO/SB/08A
Cited References (34)

P.O. Box 1247
Seattle, Washington 98111-1247
(206) 583-8888
Fax: (206) 583-8500

Substitute for form 1449A/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT <i>(use as many sheets as necessary)</i>				COMPLETE IF KNOWN		
				Application Number	09/816,869	
				Confirmation Number	6077	
				Filing Date	March 24, 2001	
				First Named Inventor	C. Andrew Neff	
				Group Art Unit	2131	
Examiner Name						
Attorney Docket No.	324628002US3					
Sheet	1	of	2			

U.S. PATENT DOCUMENTS

*EXAMINER INITIALS	Cite No.	U.S. Patent Document		Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		NUMBER	Kind Code (if known)			
	AA	5,278,753		Graft, III	1/11/94	
	AB	5,400,248		Chisholm	3/21/95	
	AC	5,495,532		Kilian et al.	2/27/96	
	AD	5,521,980		Brands	5/28/96	
	AE	5,682,430		Kilian et al.	10/28/97	
	AF	5,717,759		Micali	2/10/98	
	AG	5,864,667		Barkan	1/26/99	
	AH	5,878,399		Peralto	3/2/99	

FOREIGN PATENT DOCUMENTS

*EXAMINER INITIALS	Cite No.	Foreign Patent Document			Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T
		Office	Number	Kind Code (if known)				
	AI	WO	98/14921		Certco, LLC	4/9/98		

OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS

*EXAMINER INITIALS	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume/issue number(s), publisher, city and/or country where published.	T
	AJ	Benaloh, J., "Secret Sharing Homomorphisms: Keeping Shares of a Secret Secret", Advances in Cryptology - CRYPTO 1986, Lecture Notes in Computer Science, pp. 251-260, Springer-Verlag, Berlin, 1987	
	AK	Benaloh, J., et al., "Distributing the Power of a Government to Enhance the Privacy of Voters", ACM Symposium on Principles of Distributed Computing, pp. 52-62, 1986	
	AL	Borrell, Joan et al., "An implementable secure voting scheme", Computers & Security, Elsevier Science, Ltd., Great Britain, 1996, Vol. 15, No. 4, pp. 327-338	
	AM	Chaum, D., "Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA", EUROCRYPT 1988, pp. 177-182	
	AN	Chaum, D., "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, 24(2):84-88, 1981	
	AO	Cramer, R, et al., "A Secure and Optimally Efficient Multi-Authority Election Scheme", Advances in Cryptology - EUROCRYPT 1997, Lecture Notes in Computer Science, Springer-Verlag, 1997.	

EXAMINER

DATE CONSIDERED

* EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Substitute for form 1449A/PTO

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**

(use as many sheets as necessary)

Sheet

2

of

2

COMPLETE IF KNOWN

Application Number	09/816,869
Confirmation Number	6077
Filing Date	March 24, 2001
First Named Inventor	C. Andrew Neff
Group Art Unit	2131
Examiner Name	

RECEIVED**JUL 18 2001****Technology Center 2100**

Attorney Docket No. 32462-8002US3

OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS

*EXAMINER INITIALS	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume/issue number(s), publisher, city and/or country where published.	T
	AP	Cramer, R., et al., "Multi-Authority, Secret-Ballot Elections with Linear Work", Advances in Cryptology – EUROCRYPT 1996, Lecture Notes in Computer Science, Springer-Verlag, Berlin, 1996	
	AQ	Cramer, R., et al., "Proofs of Partial Knowledge and Simplified Design of Cryptology – CRYPTO 1994, Lecture Notes in Computer Science, pp. 174-187, Springer-Verlag, Berlin, 1994	
	AR	Cranor, Lorrie et al., "Sensus: A Security-Conscious Electronic Polling System for the Internet", Proceedings of the Hawaii International Conference on System Sciences, IEEE 1997, pp. 561-570	
	AS	Diffie, W., et al., "New Directions in Cryptography", IEEE Transactions on Information Theory, 22(6):644-654, 1976	
	AT	ElGamal, T., "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Transactions on Information Theory, IT-31(4):469-472, 1985	
	AU	Fiat, A., et al., "How to Prove Yourself: Practical Solutions to Identification and Signature Problems", Advances in Cryptology – CRYPTO 1986, Lecture Notes in Computer Science, pp. 186-194, Springer-Verlag, New York, 1987	
	AV	Fujioka, A., et al., "A Practical Secret Voting Scheme for Large Scale Elections", Advances in Cryptology – AUSCRYPT 1992, Lecture Notes in Computer Science, pp. 244-251, Springer-Verlag, 1992	
	AW	Gennaro, R., "Achieving independence efficiently and securely", Proceedings 14 th ACM Symposium on Principles of Distributed Computing (PODC 1995), New York 1995	
	AX	Iversen, K., "A Cryptographic Scheme for Computerized General Elections", CRYPTO 1991, pp. 405-419	
	AY	Jan, Jin-Ke et al., "A Secure Electronic Voting Protocol with IC Cards", Elsevier Science Inc., New York, J. Systems Software 1997, 39:93-101	
	AZ	Mu, Yi et al., "Anonymous Secure E-Voting over a Network", Proceedings, Annual Computer Security Applications Conference, IEEE 1998, pp. 293-299	
	BA	Odlyzko, A. M., "Discrete logarithms in finite fields and their cryptographic significance", Advances in Cryptology – EUROCRYPT 1984, Notes in Computer Science, Springer-Verlag, 1984	
	BB	Park, C., et al., "Efficient Anonymous Channel and All/Nothing Election Scheme", Advances in Cryptology – EUROCRYPT 1993, Lecture Notes in Computer Science, pp. 248-259, Springer-Verlag, 1993	
	BC	Pedersen, T., "A Threshold Cryptosystem without a Trusted Party", Advances in Cryptology – EUROCRYPT 1991, Lecture Notes in Computer Science, pp. 522-526, Springer-Verlag, 1991	
	BD	Sako, K., et al., "Receipt-Free Mix-Type Voting Scheme – A practical solution to the implementation of a voting booth – , EUROCRYPT 1995, pp. 393-403	
	BE	Sako, K., et al., "Secure Voting Using Partially Compatible Homomorphisms", Advances in Cryptology – CRYPTO 1994, Lecture Notes in Computer Science, Springer-Verlag, 1994	
	BF	Schnorr, C.P., "Efficient Signature Generation by Smart Cards", Journal of Cryptology, 4(3):161-174, 1991	
	BG	Schoenmakers, B., "A Simple Publicly Verifiable Secret Sharing Scheme and its Application to Electronic Voting", Advances in Cryptology – CRYPTO 1999, Lecture Notes in Computer Science, pp. 1-17, Springer-Verlag 1999	
	BH	Shamir, A., "How to Share a Secret", Communications of the ACM, 22(11):612-613, 1979	

EXAMINER

DATE CONSIDERED

* EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).